What is claimed is:

1. A random number generator comprising:

a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between signals inputted to two input units;

a delay unit for producing the phase difference between the two input signals; and

a feedback circuit for controlling the phase difference so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals is constant within a specified repetition cycle.

2. The random number generator according to claim 1, wherein the delay unit comprises a delay circuit for delaying the input signals at several stages and outputting them, and a selection circuit for selecting one of delay outputs according to a select input.

3. The random number generator according to claim 1 or 2, wherein the feedback circuit comprises:

a first counter for measuring the specified repetition cycle of the input signals;

a second counter for measuring the number of occurrences of 0 or 1 of the output from the flip-flop in every repetition cycle;

a register for holding a measurement output of the

second counter every repetition cycle;

a constant setter for generating comparison data for setting of the occurrence ratio of 0 or 1 of the output from the flip-flop;

a comparator for comparing output data of the register with the comparison data; and

a reversible counter for generating a select signal of the selection circuit on the basis of a comparison output of the comparator.

4. The random number generator according to claim 3, wherein a random number outputted from the flip-flop or a random number constructed by scrambling the former random number is used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

5. The random number generator according to claim 3, further comprising an auxiliary random number generating unit having a same structure as the random number generator as set forth in claim 3, wherein a random number from the auxiliary random number generating unit is used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

6. The random number generator according to claim 3, further comprising an auxiliary random number generating unit having a same structure as the random number generator as set forth in claim 3, wherein a random number from the auxiliary

random number generating unit and a random number constructed by scrambling a random number from the random number generator are used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

7. The random number generator according to claim 1, wherein a waveform shaping circuit is added to an input signal line of the flip-flop.

8. The random number generator according to claim 3, further comprising an initial control circuit for setting the comparison data of the comparator to 0 for a specified period when power is turned on.

9. The random number generator according to claim 1, wherein a D-type flip-flop or an R-S flip-flop is used as the flip-flop.

10. A random number generator, further comprising a plurality of the random number generators as set forth in claim 1 arranged in parallel to one another.

11. A probability generator, further comprising the random number generator as set forth in claim 1.

12. A random number generator in which a phase difference between two input signals inputted to a flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, characterized in that

a jitter generation circuit including a source for

generating a noise, an amplifier circuit for amplifying the noise, and a mixer circuit for generating jitter in the input signals by the amplified noise signal is added to an input line of the flip-flop.

13. The random number generator according to claim 12, wherein the jitter generation circuit is added to both input lines of the flip-flop.

14. The random number generator according to claim 12, wherein the jitter generation circuit is added to any one of input lines of the flip-flop, and an integration circuit for delay time correction is added to the other of the input lines.

15. The random number according to claim 12, further comprising latch means for latching an output of the jitter generation circuit every repetition cycle of the input signals.

16. A random number generator in which a phase difference between two input signals is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from a flip-flop constant, characterized in that

a phase-voltage conversion circuit for converting the phase difference between the two input signals into a voltage is added to a data input line of the flip-flop.

17. The random number generator according to claim 16, wherein the phase-voltage conversion circuit includes enable means operating only at an operation permissible time.

18. The random number generator according to claim 16, wherein a jitter generation circuit including a source for generating a noise, an amplifier circuit for amplifying the noise, and a mixer circuit for generating jitter in the input signals by the amplified noise signal is added to an output of the phase-voltage conversion circuit.

19. The random number generator according to claim 12 or 16, wherein that the jitter generation circuit includes enable means operating only at an operation permissible time.

20. The random number generator according to claim 12, wherein that the mixer circuit includes an integration circuit, and a series connection circuit of a series P-channel transistor circuit and a series N-channel transistor circuit respectively having, as inputs, the integration output signal and the amplified noise signal.

21. The random number generator according to claim 12, wherein the mixer circuit includes a series transistor circuit of an N-channel transistor and a P-channel transistor having, as an input, a combined signal of the amplified noise signal and the input signal.

22. A random number generator in which a phase difference between two input signals inputted to an R-S flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, characterized in that

a P-channel transistor is connected in series to a power supply side of an R side gate circuit or an S side gate circuit of an internal transistor circuit constituting the R-S flip-flop, an N-channel transistor is connected in series to a GND side, a source for generating a noise and an amplifier circuit for amplifying the noise are connected to inputs of the P-channel transistor and the N-channel transistor, and a threshold voltage of one of the gate circuits is changed by the amplified noise signal.

23. A random number generator in which a phase difference between two input signals inputted to an R-S flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, characterized in that

a P-channel transistor is connected in series to a power supply side of an R side gate circuit and an S side gate circuit of an internal transistor circuit constituting the R-S flip-flop, an N-channel transistor is connected in series to a GND side, a source for generating a noise and an amplifier circuit for amplifying the noise are connected to inputs of the P-channel transistor and the N-channel transistor, and threshold voltages of both of the gate circuits are changed by the amplified noise signal.

24. The random number generator according to claim 12, wherein the amplifier circuit includes a series input circuit

of a capacitor and a resistor, and a series circuit of a P-channel transistor and an N-channel transistor, and a resistor intervenes between an input and an output of the transistor circuit.

25. The random number generator according to claim 12, wherein the amplifier circuit includes a series input circuit of a capacitor and a resistor, and a series circuit of a P-channel transistor and an N-channel transistor, and a resistor and a capacitor intervene in parallel between an input and an output of the transistor circuit.

26. The random number generator according to claim 24, wherein the amplifier circuit is connected in multistage and in series.

27. The random number generator according to in claim 12, wherein the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series and short-circuiting an input and an output.

28. The random number generator according to claim 12, wherein the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series and making a resistor intervene between an input and an output.

29. The random number generator according to in claim 12, wherein that the source for generating the noise is

constructed by connecting a P-channel transistor and an N-channel transistor in series, making a resistor intervene between an input and an output, and making a series circuit of a resistor and a capacitor intervene between the input and GND.

30. The random number generator according to claim 12, wherein that the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series, making a resistor intervene between an input and an output, and making a series circuit of a resistor and a capacitor intervene between the input and a power supply.

31. The random number generator according to claim 12, wherein the source for generating the noise is constructed by short-circuiting an input and an output of an N-channel transistor, and making a resistor intervene between the output and a power supply.

32. The random number generator according to claim 12, wherein the source for generating the noise is constructed by making a resistor intervene between an input and an output of an N-channel transistor, and by making a resistor intervene between the output and a power supply.

33. The random number generator according to claim 12, wherein the source for generating the noise is constructed by short-circuiting an input and an output of a P-channel

transistor, and by making a resistor intervene between the output and GND.

34. The random number generator according to claim 12, wherein the source for generating the noise is constructed by making a resistor intervene between an input and an output of a P-channel transistor, and by making a resistor intervene between the output and GND.

35. A probability generator comprising the random number generator as set forth in claim 12.

36. A random number generator comprising:

a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between two input signals;

a phase adjustment unit for adjusting phases of the input signals; and

a feedback circuit unit for controlling the phase difference so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals converges on a given value within a specified repetition cycle,

wherein the phase adjustment unit includes coarse adjustment means of a phase and fine adjustment means operating in sequence to achieve enlargement of a phase adjustment width and shortening of a phase adjustment time.

37. The random number generator according to claim 36, wherein each of the coarse adjustment means and the fine

adjustment means includes a delay circuit for delaying the input signals at several stages and outputting them, a selection circuit for selecting one of delay outputs according to a select input, and a reversible counter for controlling the select input according to the phase difference.

38. A random number generator comprising:

a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between two input signals;

a phase adjustment unit for adjusting phases of the input signals; and

a feedback circuit unit for controlling the phase difference so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals converges on a given value within a specified repetition cycle,

wherein:

the phase adjustment unit includes a delay circuit for delaying the input signals at several stages and outputting them, a selection circuit for selecting one of delay outputs according to a select input, and a reversible counter for controlling the select input according to the phase difference,

and includes a control circuit for comparing a normal distribution of the occurrence ratio of 0 or 1 with the number

of times of occurrence of 0 or 1 within the repetition cycle and making a count number of the reversible counter variable according to a position of the normal distribution to which the number of times of occurrence corresponds to achieve shortening of the phase adjustment time.

39. The random number generator according to claim 36, further comprising an initial control circuit for making the repetition cycle shorter than the repetition cycle at a normal operation time for a given period from power activation.

40. The random number generator according to claim 36, wherein a noise generation source and a noise/phase converter are added to both input lines of the flip-flop.

41. The random number generator according to claim 36, wherein a noise generation source and a noise/phase converter are added to any one of input lines of the flip-flop.

42. A one-bit random number generator comprising:

a random number generating unit for outputting "1" and "0" as random number data;

a first counter for counting a given number of times;

a second counter of counting the number of times of occurrence of the random number data outputted from the random number generating unit to produce count data;

a register for holding the count data of the second counter in every cycle counted by the first counter; and

an output circuit for outputting the count data held in

this register as verification data.

43. The one-bit random number generator according to claim 42, further comprising, instead of the output circuit of claim 42, a comparator for comparing previously set upper limit comparison data and lower limit comparison data with the data held in the register to output a verification signal.

44. A one-bit random number generator comprising:

a random number generating unit for outputting "1" and "0" as random number data;

a data holding unit for holding previous random number data outputted from the random number generating unit;

a comparator for comparing present random number data outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other;

a counter for counting up when the count up signal is received from the comparator and clearing count when the count clear signal is received from the comparator; and

an output circuit for outputting data held in the counter as verification data.

45. A one-bit random number generator, comprising:

a random number generating unit for outputting "1" and "0" as random number data;

a data holding unit for holding previous random number data outputted from the random number generating unit;

a first comparator for comparing present random number data outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other;

a counter for counting up when the count up signal is received from the first comparator and clearing count when the count clear signal is received from the first comparator;

a register for holding output data of the counter;

a second comparator for comparing the data of the register with the output data of the counter, outputting a data overwrite signal when the latter is larger than the former, and outputting a data hold signal at a time other than that;

a control circuit for performing a control to write the output data of the counter into the register when the data overwrite signal is received from the second comparator, and to hold the data of the register when the data hold signal is received from the second comparator; and

an output circuit for outputting the data held in the register as verification data.

46. The one-bit random number generator according to

claim 45, further comprising, instead of the output circuit as set forth in claim 45, a third comparator for comparing previously set comparison data with the data held in the register to output a verification signal.

47. A one-bit random number generator comprising:

a random number generating unit for outputting "1" and "0" as random number data;

a first counter for counting a given number of times;

a data holding unit for holding previous random number data outputted from the random number generating unit;

a comparator for comparing present random number data outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other;

a second counter for counting up when the count up signal is received from the comparator and clearing count when the count clear signal is received from the comparator;

a decoder for decoding output data of the second counter to output it for respective signal lengths;

plural third counters for respectively counting output data of the decoder for the respective signal lengths;

plural registers for respectively holding output data of the respective third counters every given number of times

counted by the first counter; and

a control circuit for performing a control to output verification data from the respective registers on the basis of a signal in every given number of times counted by the first counter and output data of the comparator.

48. The one-bit random number generator according to claim 47, further comprising a selection circuit for selecting and outputting the output data of the registers.

49. A multi-pit random number generator comprising a plurality of the one-bit random number generators as set forth in claim 42 connected in parallel to each other, and a selection circuit for selecting verification data outputted from the one-bit random number generators for every bit and outputting it.

50. A multi-pit random number generator comprising a plurality of the one-bit random number generators as set forth in claim 42 connected in parallel to each other, and a selection circuit for selecting verification signals outputted from the one-bit random number generators for every bit and outputting them.

51. A probability generator comprising:

the one-bit random number generator as set forth in claim 42;

a shift register for converting random number data outputted from the one-bit random number generator from

serial data to parallel data;

a counter for counting a bit length of given parallel data;

a register for holding the parallel data of the shift register in every cycle counted by the counter; and

a comparator for comparing previously set probability upper limit data and probability lower limit data with the parallel data held in the register to output a probability signal.

52. A probability generator comprising:

the multi-bit random number generator as set forth in claim 49; and

a comparator for comparing previously set probability upper limit data and probability lower limit data with random number data outputted from the multi-bit random number generator to output a probability signal.